required for consideration of this paper are authorized to be charged in two originally-executed copies of an Amendment Transmittal Letter filed herewith.

Kindly enter the following Amendment:

IN THE CLAIMS:

Please cancel claims 83-163 without prejudice or disclaimer fo the subject matter thereof.

Please add the following new claims 164-186 as follows:

1 ~~164~~. A method for using at least one Merkle tree to authenticate revocation status about a plurality of certificates, comprising:

C1

(a) generating a plurality of values, wherein each of the values indicates that at least one of the certificates has been revoked and wherein for each certificate, there is at least one value indicating status of the certificate;

(b) constructing at least one Merkle tree containing on a plurality of its nodes at least one of the plurality of values indicating whether at least one of the certificates has been revoked; and

(c) authenticating, with a digital signature, a root node of the at least one Merkle tree to provide an authenticated root.

2 ~~165~~. A method according to claim 1 ~~164~~, wherein the digital signature is verifiable by an end user.

3 ~~166~~. A method according to claim 1 ~~164~~, wherein the values indicate which certificates have been revoked.

C1 Con't

4 ~~167~~. A method according to claim 3 ~~166~~, wherein the values include a date of revocation for the certificates that have been revoked.

5 ~~168~~. A method according to claim 1 ~~164~~, wherein the values indicate which certificates are valid.

6 ~~169~~. A method according to claim 1 ~~164~~, wherein the values include a date of issue for the certificates that have been issued.

7 ~~170~~. A method according to claim 1 ~~164~~, wherein the values indicate which certificates have been revoked and which certificates are valid.

8 ~~171~~. A method according to claim 1 ~~164~~, wherein the values indicate which certificates have been revoked and which certificates have been issued.

9 ~~172~~. A method according to claim 1 ~~164~~, wherein the values indicate which certificates are valid and which certificates have been issued.

10 ~~173~~. A method according to claim 1 ~~164~~, wherein the values indicate which certificates have been revoked, which certificates are valid, and which certificates have been issued.

11 ~~174~~. A method according to claim 1 ~~164~~, wherein at least one of the values corresponds to more than one certificate.

C1 cont

12 ~~175~~. A method according to claim 11 ~~174~~, wherein the values include a date of issue for the certificates that have been issued.

13 ~~176~~. A method according to claim 1 ~~164~~, wherein certificate information determines locations of the values within the Merkle tree.

14 ~~177~~. A method according to claim 1 ~~164~~, wherein positions of the values within the Merkle tree provide information about certificates corresponding thereto.

15 ~~178~~. A method according to claim 14 ~~177~~, wherein the information includes serial numbers for each of the certificates.

16 ~~179~~. A method according to claim 1 ~~164~~, wherein the values correspond to serial numbers of the certificates.

17 ~~180~~. A method according to claim 16 ~~179~~, wherein the certificate values correspond to serial numbers of the certificates combined with additional information.

18 ~~181~~. A method according to claim 1 ~~164~~, wherein the authenticated root contains additional information.

C1 cont

19 ~~182~~. A method according to claim 18 ~~181~~, wherein the additional information includes date information.

20 ~~183~~. A method according to claim 18 ~~181~~, wherein the additional information includes an indication of at least one of: revoked, issued, and valid for describing certificate information corresponding to the values of the Merkle tree.

21 ~~184~~. A method according to claim 1 ~~164~~, wherein the values indicating status of certificates are leaf nodes of the Merkle tree.

22 ~~185~~. A method, according to claim 1 ~~164~~, further comprising:

introducing dummy items.

23 ~~186~~. A method, according to claim 22 ~~185~~, wherein the number of dummy items that is introduced plus the number of other items is a power of two.